Quanto è sicuro il vostro hypervisor?

Architettura e sicurezza: le due parole chiave

Peter Hoogenboom
Engineering manager
Green Hills Software

Una delle ragioni più importanti per usare la virtualizzazione, specialmente nelle applicazioni embedded, è poter eseguire più programmi nei rispettivi ambienti operativi, separati in modo sicuro l'uno dall'altro. Le applicazioni più sicure possono essere dapprima eseguite in un'area protetta (sandbox). In teoria, solamente l'ambiente operativo ospite che gira nell'ambiente di prova è vulnerabile agli attacchi maligni provenienti dal mondo esterno.
In pratica, succede che l'architettura sottostante dell'hypervisor determina se è possibile ottenere la separazione dei vari ambienti nel modo desiderato.
I più diffusi hypervisor commerciali sono basati su un'architettura monolitica (Fig. 1). In questo caso esiste un solo hypervisor, che coordina tutti gli ambienti virtuali di prova, ognuno dei quali esegue il proprio sistema operativo ospite. L'hypervisor viene eseguito come parte del sistema operativo nativo monolitico, affiancato dai device driver, dal file system e dallo stack di comunicazione, completamente all'interno dello spazio del kernel.
Ciò significa che all'hypervisor vengono concessi i privilegi della CPU necessari per accedere a tutte le risorse di I/O e di memoria. Dal punto di vista della sicurezza questa non è una buona architettura.
Una sola vulnerabilità all'interno dell'hypervisor potrebbe consentire a un hacker di ottenere l'accesso all'intero sistema, compresi tutti i sistemi operativi ospiti.
L'architettura a microkernel, invece, è stata progettata specificatamente per garantire una separazione affidabile tra le partizioni delle applicazioni (Fig. 2). Con questa architettura i complessi programmi per la virtualizzazione sono confinati nello spazio utente. In questo modello, quindi, ogni sistema operativo ospite utilizza la propria istanza del programma di virtualizzazione, così che le varie macchine virtuali rimangono effettivamente separate tra loro. Un attacco a un hypervisor di uno dei sistemi operativi ospiti può compromettere una macchina virtuale, ma non l'intero sistema o un'altra macchina virtuale. Il kernel è il solo componente che lavora nello spazio kernel.

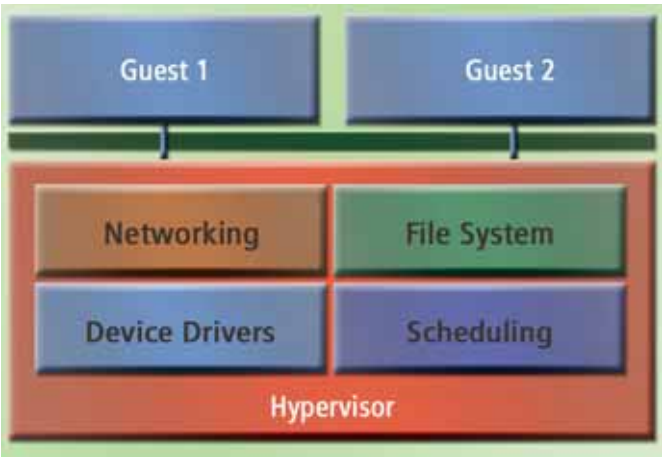

Fig. 1 - Hypervisor monolitico

"Fuga" dall'ambiente isolato

Alcune ricerche pubblicate di recente hanno dimostrato che la sicurezza degli hypervisor può essere compromessa. Nel 2006 il progetto Subvirt ha dimostrato la fattibilità di rootkit che mettono a rischio sia VMware, sia VirtualPC. Il progetto Bluepill, avviato dall'esperta di sicurezza polacca Joanna Rutkowska, è andato un passo oltre a ha dimostra-

to che un programma malware può iniziare ad agire da proprio hypervisor sotto Windows. Tavis Ormandy, di Google, ha scoperto debolezze in QEmu, VMware, Bochs e in altri hypervisor meno conosciuti, dimostrando come sia possibile uscire dai limiti imposti dagli ambienti virtuali teoricamente separati.

Profilo di protezione

Quindi, per le applicazioni critiche dal punto di vista della sicurezza, non si può fare affidamento sulle affermazioni dei fornitori di hypervisor e di sistemi operativi. Affinché i consumatori, le aziende e gli enti governativi possano confrontare i prodotti informatici dedicati alla sicurezza che intendono acquistare, diverse organizzazioni nazionali si sono alleate formando un'organizzazione internazionale chiamata Common Criteria for IT Security Evaluation, che è gestita dall'associazione statunitense NIAP (National Information Assurance Partnership). Common Criteria ha definito un corrispondente schema di valutazione e validazione (CCEVS) per varie categorie di prodotti, come database, smartcard e così via. È quindi consigliabile leggere prima i report di valutazione, pubblicati da un laboratorio di prova indipendente CCTL (Common Criteria Test Laboratory), relativi al prodotto che si intende acquistare. Prima di cominciare a valutare un prodotto informatico è necessario descrivere "da cosa dovete proteggervi e in quali condizioni". Questo è un "profilo di protezione" o PP (Protection Profile) e spesso serve come indicatore della robustezza che ci si può aspettare da un prodotto.

"Bunker" senza collegamento a Internet

Ogni prodotto informatico che cerca di soddisfare i requisiti definiti in un certo profilo di protezione ha un certo livello di valutazione delle garanzie o EAL (Evaluation Assurance Level). Si tratta di un valore numerico che informa l'acquirente quanto sia certo che il prodotto effettivamente garantisca la protezione descritta dal profilo di protezione. Il livello EAL1 è il più basso e il livello EAL7 è quello più alto. Più alto è il livello, più sono le prove e i metodi di verifica richiesti per ottenerlo. Ovviamente, un profilo di protezione che richiede un alto grado di robustezza ha senso solo per quei prodotti informatici che devono essere valutati a un livello EAL elevato (almeno 6). A questi livelli, una dichiarazione del produttore che riguarda la sicurezza di un prodotto informatico può essere valutata da un laboratorio di prova indipendente accreditato dall'associazione NIAP. Il certificato ottenuto, riferito ai criteri e ai livelli PP/EAL utilizzati, permette di confrontare equamente i vari prodotti informatici.

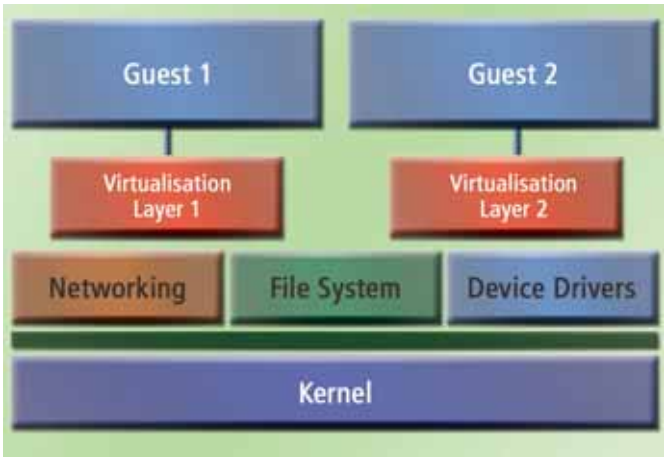

Fig. 2 - Hypervisor basato su microkernel

Esistono attualmente diversi profili di protezione definiti in ambito CCEVS per i sistemi operativi. I più comuni sono il profilo CAPP (Controlled Access Protection Profile) e il profilo SKPP (Separation Kernel Protection Profile). NIAP pubblica sul suo sito una lista dei sistemi operativi che hanno ottenuto un certificato e di quelli in corso di valutazione. Il profilo CAPP presuppone che il sistema lavori in un ambiente non ostile e che vi protegga da tentativi occasionali o involontari di violazione dei sistema di sicurezza. Si tratta di un livello accettabile per un prodotto informatico che lavora in un "bunker" senza alcun collegamento in rete con l'esterno.

Il profilo SKPP richiede che il sistema operativo contenga servizi di sicurezza e contromisure adatte a neutralizzare attacchi (o accessi non autorizzati) provenienti, per esempio, da una connessione di rete. Il profilo SKPP richiede anche che il sistema operativo supporti la stretta ed effettiva separazione tra i domini, compresa la separazione temporale dell'elaborazione a diversi livelli di sicurezza (periods processing) e l'assenza di canali di comunicazione nascosti (covert channels). Inoltre, i requisiti del profilo SKPP impongono l'uso di metodi formali per provare matematicamente la correttezza delle politiche di sicurezza, la formalizzazione delle specifiche, sistemi di comunicazione formali tra progettazione e realizzazione, completa copertura delle prove su tutti i requisiti funzionali e prove di penetrazione da parte dell'agenzia statunitense NSA, con accesso completo al codice sorgente.